Margaret Bilu
Office 604

bilu@cims.nyu.edu

Algebra homework 10
Index, Lagrange's theorem, normal subgroups

Exercise 1. Compute the indexes of the following subgroups H_i of the following groups G_i.

1. $H_1 = \langle 3 \rangle$ (subgroup generated by 3) in $G_1 = \mathbf{Z}/81\mathbf{Z}$.

   Solution. You can compute the index using the counting formula, by first computing the order of H_1. We have
   $$H_1 = \{0,\ 1\cdot 3,\ 2\cdot 3, \ldots,\ 26\cdot 3\}$$
   so $|H_1| = 27$, and therefore
   $$[G_1 : H_1] = \frac{|G_1|}{|H_1|} = \frac{81}{27} = 3.$$
   In general, you can remember that $\mathbf{Z}/n\mathbf{Z}$ has a unique group of order d (and index n/d) for every divisor d of n, namely $\langle \frac{n}{d} \rangle$. Thus, here, since $3 = 81/27$, we have that $\langle 3 \rangle$ is of order 27 and index 3.

2. $H_2 = 23\mathbf{Z}$ in $G_2 = \mathbf{Z}$.

   Solution.

   The cosets correspond to the 23 possible remainders of the Euclidean division by 23. Hence, $[G_2 : H_2] = 23$.

3. $H_3 = \{\mathrm{id}, (1,2,3), (1,3,2)\}$ in $G_3 = \mathfrak{S}_3$.

   Solution.

   The index of H_3 in G_3 is given by the counting formula:
   $$[G_3 : H_3] = \frac{|G_3|}{|H_3|} = \frac{6}{3} = 2$$

4. $H_4 = \{\mathrm{id}, (1,3)\}$ in $G_4 = \mathfrak{S}_3$.

   Solution.

   The index of H_4 in G_4 is given by the counting formula:
   $$[G_4 : H_4] = \frac{|G_4|}{|H_4|} = \frac{6}{2} = 3$$

Exercise 2. Let $f : \mathbf{Z}/9\mathbf{Z} \to \mathbf{Z}/9\mathbf{Z}$ given by $f(x) = 3x$.

1. Prove that f is a group homomorphism.

   Solution.

   f is clearly well-defined. Let $x, y \in \mathbf{Z}/9\mathbf{Z}$. We have:
   $$f(x+y) = 3(x+y) = 3x + 3y = f(x) + f(y)$$
   This is true for any x, y. As a consequence f is a homomorphism.

2. Compute $\operatorname{Ker} f$ and $\operatorname{Im} f$.

   Solution.

   By definition, $\operatorname{Ker} f = \{x \in \mathbf{Z}/9\mathbf{Z} : 3x = 0\} = \{0, 3, 6\}$.

   $\operatorname{Im} f = \{3x : x \in \mathbf{Z}/9\mathbf{Z}\} = \{0, 3, 6\}$.

3. Check that $[\mathbf{Z}/9\mathbf{Z} : \operatorname{Ker} f] = |\operatorname{Im} f|$.

   Solution. The kernel has three cosets $\{0, 3, 6\}$, $\{1, 4, 7\}$, $\{2, 5, 8\}$, so it is of index 3. The image is of order 3, so the formula indeed holds.

Exercise 3. 1. Give a list of all the subgroups of $\mathbf{Z}/14\mathbf{Z}$ together with their orders.

   Solution.

   The order of a subgroup of $\mathbf{Z}/14\mathbf{Z}$ must divide 14. Therefore, non trivial subgroups can be of order 2 or 7. Moreover, we know from lectures that for every divisor d of 14, there is a unique subgroup of order d, namely the one generated by $\frac{14}{d}$. Thus, the only subgroups other than $\{0\}$ and $\mathbf{Z}/14\mathbf{Z}$ are $\langle 2\rangle = \{0, 2, 4, 6, 8, 10, 12\}$ of order 7 and $\langle 7\rangle = \{0, 7\}$ of order 2.

2. Check that

$$14 = \sum_{d|14} \phi(d)$$

   where ϕ is Euler's function.

   Solution.

   By definition of the Euler function, we have $\phi(14) = 6$, since 1, 3, 5, 9, 11, 13 are relatively prime to 14, $\phi(1) = 1$, $\phi(2) = 1$, $\phi(7) = 6$.

   Therefore the formula is satisfied on this example: $14 = \phi(1) + \phi(2) + \phi(7) + \phi(14)$.

Exercise 4. Let $\phi : G \to G'$ be a group homomorphism. Assume that G is of order 18, G' is of order 15 and that ϕ is not the trivial homomorphism. What is the order of $\operatorname{Ker}\phi$?
Solution.
As seen in lectures, $|\operatorname{Ker}\phi| \times |\operatorname{Im}\phi| = |G| = 18$.
Let's analyze the order of the image. It's a subgroup of G' and therefore, by Lagrange's theorem, $|\operatorname{Im}\phi|$ divides 15. So it's either 3, 5 or 15 (1 is excluded since ϕ is not trivial.).
It can't be 5 nor 15 since $|\operatorname{Ker}\phi| \times |\operatorname{Im}\phi| = 18$ implies that $|\operatorname{Im}\phi|$ is also a divisor of 18.
Therefore, $|\operatorname{Im}\phi| = 3$, and it follows that $|\operatorname{Ker}\phi| = \frac{18}{3} = 6$.

Exercise 5. 1. Find an integer x such that $x^2 \equiv -1 \pmod 5$.

   Solution.

   Observe that $3^2 \equiv -1 \pmod 5$.

2. Find an integer x such that $x^2 \equiv -1 \pmod{13}$.

   Solution.

   Observe that $5^2 \equiv -1 \pmod{13}$.

3. Let p be a prime congruent to 3 modulo 4. Show that there is no solution to the equation $x^2 \equiv -1 \pmod p$.

   Solution.

   Assume there exists x such that $x^2 \equiv -1 \pmod p$. The integer $p - 1$ is even, so we may raise both sides to the power $\frac{p-1}{2}$. On the left-hand side we get $(x^2)^{\frac{p-1}{2}} = x^{p-1}$, which by Fermat's little theorem should be congruent to 1 modulo p. On the right-hand side we get $(-1)^{\frac{p-1}{2}}$: since p is of the form $3 + 4k$ for some integer k, we get that $\frac{p-1}{2} = 1 + 2k$ is odd, so that $(-1)^{\frac{p-1}{2}} = -1$. We therefore get $1 \equiv -1 \pmod p$, which implies that p divides 2, which is impossible.

Exercise 6. For every integer $n \geq 0$, show that 13 divides $11^{12n+6} + 1$.

Solution. By Fermat's little theorem, $11^{12} \equiv 1 \pmod{13}$. Thus, for every $n \geq 0$, $11^{12n} \equiv 1 \pmod{13}$. Now, we have $11 \equiv -2 \pmod{13}$, so $11^2 \equiv 4 \pmod{13}$, so $11^4 \equiv 3 \pmod{13}$, and, multiplying the last two congruences, $11^6 = 11^2 \times 11^4 \equiv 4 \times 3 \equiv -1 \pmod{13}$. Thus, we have $11^{12n+6} \equiv -1 \pmod{13}$, whence the result.

Exercise 7. Find the remainder of 11^{1213} in the Euclidean division by 26.

Solution. You can check that $\phi(26) = 12$, so by Euler's theorem, since 11 is relatively prime to 26,

$$11^{12} \equiv 1 \pmod{26}.$$

Now, $1213 \equiv 1 \pmod{12}$, so $11^{1213} \equiv 11 \pmod{26}$. The remainder is 11.

Exercise 8. Let G be a group and H, K normal subgroups of G. Show that $H \cap K$ is a normal subgroup of G.

Solution. We first prove that $H \cap K$ is a subgroup of G.
Closure: Let $x, y \in H \cap K$. Then x, y are elements of H and of K. By closure of H and K, xy is an element of H and of K, so of $H \cap K$.
Identity: We have $e \in H$ and $e \in K$, so $e \in H \cap K$.
Inverses: Let $x \in H \cap K$. Then $x \in H$, so $x^{-1} \in H$, and $x \in K$, so $x^{-1} \in K$. Thus $x^{-1} \in H \cap K$.
We now prove $H \cap K$ is normal. Let $x \in H \cap K$ and let $g \in G$. Then since $x \in H$ and H is normal, we have $gxg^{-1} \in H$. Since $x \in K$ and K is normal, we have $gxg^{-1} \in K$. Thus $gxg^{-1} \in H \cap K$, so $H \cap K$ is normal.